Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 5 | May 2017

SECURITY ISSUES IN CLOUD COMPUTING

Supreet Kaur [1] | Amanpreet Singh [2]

[1] Assistant Professor, Department of Computer Science.

[2] Assistant Professor, Department of Computer Science and Engineering.

ABSTRACT

Cloud computing is model which uses combine concept of "software-as-a-service" and "utility computing", provide convenient and on-demand services to requested end users. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud computing is architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Using of cloud computing, the software programs aren't run from one's personal computer, but are rather stored on servers accessed via the Internet.

KEYWORDS: Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform.

1. INTRODUCTION

Cloud computing is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts [1]. Cloud Computing provides resources and capabilities of Information Technology (e.g., applications, storages, communication, collaboration, infrastructure) via services offered by CSP (cloud service provider). Cloud Computing has various characteristics as shared infrastructure, self-service, pay-per use model, dynamic and virtualized, elastic and scalable. Cloud computing has the capacity of scaling and elasticity which is perfect for such an environment.

A cloud computing offer companies an increased storage than traditional storage systems. Software updates and batches are highly automated with reduced number of hired highly skilled IT personnel [2].

The architecture of the Cloud Computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate. When it comes to cloud it is more focused upon the frontend and the back end. The front end is the User who requires the data, whereas the backend is the numerous data storage device, server which makes the Cloud [3].

Cloud Computing

1.1 Characteristics Of Cloud Computing:

- **High scalability**

Cloud environments enable servicing of business requirements for larger audiences, through high scalability.

- **Agility**

The cloud works in the 'distributed mode' environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness)

- **High availability and reliability**

Availability of servers is high and more reliable as the chances of infrastructure failure are minimal.

- **Multi-sharing**

With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.

2. SECURITY ISSUES IN CLOUD SERVICES

Cloud computing service models are SAAS, PAAS and IAAS, which provides software as a service, platform as a services and infrastructure as a service to end users or customers. These three service models are built on top of each other, as shown in Fig. 1; as a result their capabilities are inherited as well as security issues and risks.

So, service providers are not be able to take care only part of it, rather than as a whole to provide secure environment. In this part of this paper clearly indicate major security issues based on these service models and what needs to be addressed by implementing appropriate countermeasures.

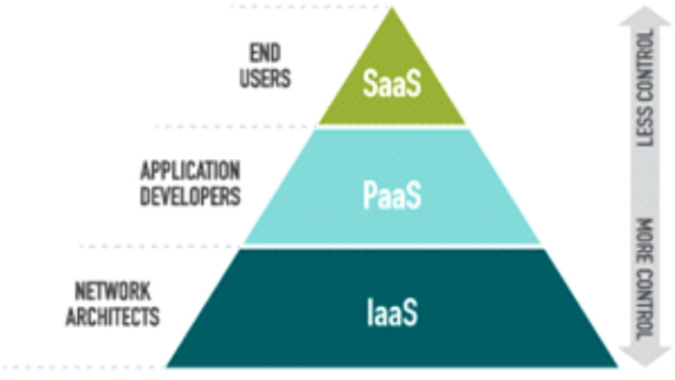

Fig: 1

2.1 Security Issues In SAAS:

In Software as a Service (SAAS) model, the client has to depend on the service provider for proper security measures. The provider must ensure that the multiple users don't get to see each other's data. So, it becomes important to the user to

ensure that right security measures are in place and also difficult to get an assurance that the application will be available when needed [4]. As a result, there are some securities issues arise such as: how is being data stored and where, what types of security is being provided for data manipulation and storage. There are some key security basics need to be considered during SAAS deployment and development. These are:

- **Data Security:**

Data control over cloud services make difficult to protect and enforce identity theft and cybercrime security. Sharing resources across multiple domains and failures of data backup also arise some data leakage.

- **Network Security:**

In cloud environment data are being transferred over the Internet, thus data flow security is an important issue to avoid leakage of information. To sniff network packets an intruder can make use of data packet to analyze weakness in network security configuration. Attackers can gain access applications and data through hacking such as: some kind of remote access mechanism and injection (SQL and some bad command) vulnerabilities. DoS (Denial of Service), DDoS (Distributed DoS), man in the middle attacks, social networking attacks and some unauthorized attacks creates grate security issues in cloud.

- **Data Confidentiality:**

Privacy and confidentiality issues are taking placed when data shares between various users, devices and applications.

2.2 Security Issues In PAAS:

Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher-level services. The PaaS model may be hosted on top of IaaS model or on top of the cloud infrastructures directly. Google Apps and Microsoft Windows Azure are the most known PaaS. The PaaS model is based on the Service oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks [5].

2.3 Security Issues In IAAS:

Infrastructure as a service (IaaS): Cloud computing providers offer physical and virtual computers, extra storage networking devices etc. The virtual machines are run by hypervisors that is organized into pools and controlled by operational support systems. It is cloud users responsibilities to install operating system images on the virtual machines as well as their application software.

Cloud computing combines virtualization technologies are creative way to provide better IT services to consumers. Due to rising virtualization technology poses some security issues for control over the owner of data regardless of physical location. Various security issues are arising to deploy models in IaaS. Private cloud environment creates fewer security risks compared to public cloud. The cloud concept implemented just over the Internet, so whatever security issues and threats are facing in the Internet, for cloud services need to consider as well. Infrastructure is not only appropriate for hardware resources, where data is being reside or processed, but also the way data are being transmitted over the media from source to destination over the open network. There are some possibilities that data can be routed through intruder's network or infrastructure [6, 7].

Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high-performance computing applications.

3. SOLUTIONS AND TIPS TO COLUD SECURITY ISSUES

There is need for advanced and extended technologies, concepts and methods that provide secure server which leads to a secure cloud.

Data Security and Control: The service providers should have enough skills to prevent, detect and react according to various security breaches. Service logs and service agreement terms inspections are performed regularly. However, there are some validity tests also required for companies to avoid security breach because of malicious data are in cloud such as: cross-sire scripting, insecure configuration, SQL injection flaws and weakness in access control inside companies policies. Data in cloud environment should be identified and classified according to their types. Service providers should provide transparent services (controls, security and operations) for clients.

Network Security: Service providers also need to do some tests and validate network security by using some prominence security tools such as: SSL, session management and packet analysis to avoid hijacking active session and access clients' credential data. For a secure system to prevent unauthorized modification and access to data by using adequate set up or configuration of firewall and auditable access rights. To secure data traffic, some policies should be implemented in router and layer three switch.

Access Control: To generate trusted user profiles based on their definitions and roles. Identity management and access security mechanism should be implemented and monitored according to their regular schedule. Service providers should prove that they have adequate security mechanism to protect unauthorized access. All access or changes in cloud services (resources and data) ought to provide auditable report whether it is success or fail and review along with monitoring to be performed regular basis.

Data Confidentiality and Integrity: Proper authentication and authorization mechanism should implement to protect illegal disclose and modification of data. Network service providers must be able to monitor network load or traffic for proper load balancing and data distribution over network. Service development and deployment models must be clear for a developer to protect and restrict use of data.

Security parameters are appropriately defined for data segregation and secure cryptographic methods and properties should be implemented in control manner such as: for secure key transfer can be used RAS and for encryption key size should be consider according to their priority of data security or uses. Data replication and backup policies are also need to be standard and provided auditable proof for data restore procedures, which includes accuracy and completeness over time.

REFERENCES

[1] Michael glas and paul Andres, "An Oracle white paper in enterprise architecture achieving the cloud computing vision", CA-U.S.A, Oct 2010.

[2] "IT-3_Cloud_Computing" A news Letter for IT professionals Issue 3 2012.

[3] Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.

[4] Choudhary V.(2007). Software as a service: implications for investment in software development. In International conference on system sciences, 2007, p. 209.

[5] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore 2009, pp. 109-116.

[6] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, July 2010.

[7] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, 2011.